Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

  - **Multiple Vendors Linux Kernel routing_ioctl() Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Denial of Service & Information Disclosure (Updated)**
  - **Multiple Vendors Linux Kernel USB Subsystem Denials of Service (Updated)**
  - Multiple Vendors Linux Kernel Denials of Service
  - **Multiple Vendors Linux Kernel Console Keymap Arbitrary Command Injection (Updated)**
  - **Multiple Vendors Linux Kernel PTrace 'CLONE_THREAD' Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PTraced Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Management Denials of Service (Updated)**
  - **Multiple Vendors Linux Kernel World Writable SYSFS Information Disclosure (Updated)**
  - **Multiple Vendors SpamAssassin Spam Detection Bypass (Updated)**
  - Multiple Vendors Linux Kernel IPv6 FlowLable Denial of Service
  - Multiple Vendors Linux Kernel POSIX Timer Cleanup Handling Local Denial of Service
  - **Multiple Vendors Kerberos V5 Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel SNMP Handler Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Resource Leak Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel ISO File System Remote Denial of Service (Updated)**
  - **Linux Kernel ZLib Invalid Memory Access Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel SCSI ProcFS Denial of Service (Updated)**
  - Multiple Vendors Apache MPM 'Worker.C' Remote Denial of Service
  - **Multiple Vendors NetPBM PNMToPNG Remote Buffer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel Information Disclosure (Updated)**
  - **Multiple Vendors Perl 'miniserv.pl' script Format String (Updated)**
  - **Opera Web Browser Arbitrary Command Execution (Updated)**
  - **PHPMyAdmin Cross-Site Scripting (Updated)**
  - PHPMyAdmin 'Import_Blacklist' Variable Overwrite
  - **phpMyAdmin Local File Inclusion & Cross-Site Scripting (Updated)**
  - SAMEDIA Landshop Multiple SQL Injection
  - Sun Communications Services Delegated Administrator Default Password Disclosure
  - SUSE Linux Squid Proxy SSL Handling Remote Denial of Service
  - **Sylpheed LDIF Import Buffer Overflow (Updated)**
  - Open Motif libUil Buffer Overflows
  - **UW-imapd Denial of Service and Arbitrary Code Execution (Updated)**
- Multiple Operating Systems
  - 1-Script 1-Search Cross-Site Scripting
  - 88Scripts Event Calendar Index.PHP SQL Injection
  - Alisveristr E- Multiple SQL Injection
  - FileLister Cross-SIte Scripting
  - Apple Quicktime/iTunes Heap Overflow
  - Atlantis Knowledge Base Software SQL Injection
  - Atlassian Confluence Cross-Site Scripting
  - Avaya TN2602AP IP Media Resource 320 Remote Denial of Service
  - Check Point VPN-1 SecureClient Policy Bypass
  - **Cisco IPSec IKE Traffic Remote Denial of Service (Updated)**
  - **Cisco IOS HTTP Service HTML Injection (Updated)**
  - DoceboLMS Directory Traversal & File Upload
  - DotClear SQL Injection
  - Drupal Multiple Vulnerabilities
  - DuWare DuPortalPro Cross-Site Scripting
  - e107 Website System Redirection & Voting Manipulation
  - **eFiction Input Validation (Updated)**
  - Extreme Corporate Cross-Site Scripting
  - FAQRing SQL Injection
  - FastJar Archive Extraction Directory Traversal
  - FFmpeg Remote Buffer Overflow
  - PHPYellowTM Multiple SQL Injection
  - Hobosworld HobSR Multiple SQL Injection
  - Horde IMP Email Attachments HTML Injection
  - **Horde Error Message Cross-Site Scripting (Updated)**
  - **Inkscape 'ps2epsi.sh' Insecure Temporary File (Updated)**
  - Instant Photo Gallery SQL Injection
  - Java Search Engine Cross-Site Scripting
  - **Mambo Open Source Remote File Include (Updated)**
  - MediaWiki User Language Remote Code Execution
  - Mr CGI Guy Multiple Software Search.CGI Cross-Site Scripting
  - Multiple Vendor BIOS Password Persistence Weakness
  - **Multiple Vendors Inkscape SVG Image Buffer Overflow (Updated)**
  - **Multiple Vendors Lynx URI Handlers Arbitrary Command Execution (Updated)**
  - **Multiple Vendors Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows (Updated)**
  - **Multiple Vendors IPSec ESP Packet Modification (Updated)**
  - **Multiple Vendors PHP Group Exif Module Remote Denial of Service (Updated)**
  - **Multiple Vendors Lynx 'HTrjis()' NNTP Remote Buffer Overflow (Updated)**
  - MultiTech MultiVOIP Remote Buffer Overflow
  - MXChange Unspecified Cross-Site Scripting & SQL Injection

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source

Absolute Shopping Package Solutions Shopping Cart Professional 2.9d, Lite 2.1	Multiple vulnerabilities have been reported in Shopping Cart that could let remote malicious users conduct Cross-Site Scripting or execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Absolute Shopping Package Solutions Shopping Cart Cross-Site Scripting CVE-2005-4003	High	Security Focus, ID: 15694, December 3, 2005
Alan Ward A-FAQ 1.0	Multiple vulnerabilities have been reported in A-FAQ that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	A-FAQ SQL Injection CVE-2005-4064	Medium	Security Focus, ID: 15741, December 6, 2005
ASP-DEV ASP Resources Forum	An input validation vulnerability has been reported in ASP Resources Forum that could let remote malicious users perform SQL Injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	ASP Resources Forum SQL Injection	Medium	Security Tracker, Alert ID: 1015316, December 6, 2005
Cisco Cisco Security Agent 4.5.0, 4.5.1	A vulnerability has been reported in Cisco Security Agent that could let local malicious users obtain elevated privileges. A vendor solution is available: http://www.cisco.com/warp/public/707/cisco-sa-20051129-csa.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco Security Agent Elevated Privileges CVE-2005-3886	Medium	Cisco, Security Advisory cisco-sa-20051129-csa, November 29, 2005
Citrix Systems Citrix MetaFrame Secure Access Manager 2.0 to 2.2, Citrix NFuse Elite 1.0	An input validation vulnerability has been reported in Citrix MetaFrame Secure Access Manager that could let remote malicious users conduct Cross-Site Scripting. A vendor solution is available: http://support.citrix.com/article/CTX108208 There is no exploit code required.	Citrix MetaFrame Secure Access Manager and NFuse Elite Cross-Site Scripting CVE-2005-3971	Medium	Citrix, CTX108208, November 29, 2005
IISWorks ASPKnowledgeBase	A vulnerability has been reported in ASPKnowledgeBase that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	IISWorks ASPKnowledge Base Cross-Site Scripting CVE-2005-4047	Medium	Security Focus, ID: 15734, December 6, 2005
infinetSoftware MyTemplateSite 1.2 and prior	A vulnerability has been reported in MyTemplateSite ('search.asp'), that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	MyTemplateSite Cross-Site Scripting CVE-2005-4004	Medium	Security Focus, ID: 15693, December 3, 2005
IPswitch IMail Server 8.20, Collaboration Suite 2.0	Multiple vulnerabilities have been reported in IMail Server and Collaboration Suite that could let remote malicious users cause a Denial of Service or execute arbitrary code. A vendor solution is available: IMail Server: http://www.ipswitch.com/support/imail/releases/imail_professional/im822.asp Collaboration Suite http://www.ipswitch.com/support/ics/updates/ics202.asp There is no exploit code required.	Ipswitch IMail Server IMAP and SMTP Service Two Vulnerabilities CVE-2005-2923 CVE-2005-2931	High	Security Focus, ID: 15752, 15753, December 6, 2005

MailEnable Professional 1.6, Enterprise 1.1	A vulnerability has been reported in MailEnable that could let remote malicious users cause a Denial of Service. A vendor solution is available: http://www.mailenable.com/hotfix/ Currently we are not aware of any exploits for this vulnerability.	MailEnable Denial of Service CVE-2005-3993	Low	Secunia, Advisory: SA17820, December 2, 2005
Microsoft Internet Explorer 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users disclose information. Specifically, importing CSS files may allow for cross domain security restriction bypassing. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Microsoft Internet Explorer Information Disclosure CVE-2005-4089	Medium	Security Focus, ID: 15660, December 01, 2005
Microsoft Windows	A vulnerability has been reported in Windows that could let local malicious users perform a Denial of Service. *NOTE: This issue has been disputed by third parties.* No workaround or patch available at time of publishing. An exploit has been published.	Microsoft Windows CreateRemote Thread Denial of Service CVE-2005-3981	Low	Security Focus, ID: 15671, December 01, 2005
NetAuctionHelp Auction Software 3.0 and prior	Multiple vulnerabilities have been reported in NetAuctionHelp Auction Software that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	NetAuctionHelp Auction Software Cross-Site Scripting CVE-2005-4063	Medium	Security Focus, ID: 15737, December 6, 2005
RainWorx rwAuctionPro 4.0 and prior	A vulnerability has been reported in rwAuctionPro that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	rwAuction Pro Cross-Site Scripting CVE-2005-4060	Medium	Secunia Advisory: SA17905, December 6, 2005
SiteBeater SiteBeater MP3 Catalog 2.0.3 and prior	A vulnerability has been reported in SiteBeater MP3 Catalog ('search.asp'), that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	SiteBeater MP3 Catalog Cross-Site Scripting CVE-2005-3999 CVE-2005-4000	Medium	Secunia, Advisory: SA17856, December 5, 2005
SiteBeater SiteBeater News System 4.0 and prior	A vulnerability has been reported in SiteBeater News System (archive.asp'), that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	SiteBeater News System Cross-Site Scripting CVE-2005-4000	Medium	Secunia, Advisory: SA17857, December 5, 2005
Soulpress News 1.0 and prior	A vulnerability has been reported in Soulpress News ('search.asp'), that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Solupress News Cross-Site Scripting CVE-2005-3998	Medium	Secunia, Advisory: SA17854, December 5, 2005
Symantec pcAnywhere 11.5.1, 11.5 and prior	A vulnerability has been reported in pcAnywhere the could let remote malicious users perform a Denial of Service. A vendor solution is available: http://www.symantec.com/avcenter/security/Content/2005.11.29.html	pcAnywhere Authentication Denial of Service Vulnerability CVE-2005-3934	Low	Symantec, SYM05-026, November 29, 2005

	Currently we are not aware of any exploits for this vulnerability.			
XCent XcClassified 3.0 and prior	A vulnerability has been reported in XcClassified that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	XcClassified Cross-Site Scripting CVE-2005-4062	Medium	Secunia Advisory: SA17903, December 6, 2005
XCent XcPhotoAlbum 1.0	A vulnerability has been reported in XcPhotoAlbum that could let remote malicious users perform Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required.	XcPhotoAlbum Cross-Site Scripting CVE-2005-4061	Medium	Secunia Advisory: SA17904, December 6, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Appfluent Technology Database IDS 2.0	A buffer overflow vulnerability has been reported in the 'APPFLUENT_HOME' environment variable when handling a malformed value, which could let a malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Appfluent Technology Database IDS Buffer Overflow CVE-2005-4076	High	Security Focus, Bugtraq ID: 15755, December 7, 2005
Astaro Internet Security Astaro Security Linux 6.1 01, 6.0 02, 6.0 01	A remote Denial of Service vulnerability has been reported when handling malformed IKE traffic. Updates available at: http://www.astaro.org/showflat.php?Cat=&Number=63958&page=0&view=collapsed&sb=5&o=&fpart=1#63958 Vulnerability can be reproduced using the PROTOS ISAKMP Test Suite.	Astaro Security Linux ISAKMP IKE Traffic Denial of Service CVE-2005-3985	Low	Security Focus, Bugtraq ID: 15666, December 1, 2005
Daniel Stenberg curl 7.12-7.15, 7.11.2	A buffer overflow vulnerability has been reported due to insufficient bounds checks on user-supplied data before using in a finite sized buffer, which could let a local/remote malicious user execute arbitrary code. Upgrades available at: http://curl.haxx.se/download/curl-7.15.1.tar.gz Currently we are not aware of any exploits for this vulnerability.	cURL / libcURL URL Parser Buffer Overflow CVE-2005-4077	High	Security Focus, Bugtraq ID: 15756, December 7, 2005
Easy Search System Easy Search System 1.1	A Cross-Site Scripting vulnerability has been reported in 'search.cgi' due to insufficient sanitization of the 'q' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	Easy Search System Cross-Site Scripting CVE-2005-4032	Medium	Security Focus, Bugtraq ID: 15705, December 5, 2005
Edgewall Software Trac 0.9	An SQL injection vulnerability has been reported in the ticket query module due to insufficient sanitization of the 'group' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://projects.edgewall.com/trac/wiki/TracDownload There is no exploit code required; however, a Proof of Concept exploit script has been published.	Edgewall Trac SQL Injection CVE-2005-3980	Medium	Security Tracker Alert ID: 1015302, December 1, 2005

Edgewall Software Trac 0.9.1, 0.9, 0.8.1- 0.8.4, 0.7.1	An SQL injection vulnerability has been reported in the search module due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://ftp.edgewall.com/pub/trac/trac-0.9.2.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	Edgewall Software Trac Search Module SQL Injection CVE-2005-4065	Medium	Security Focus, Bugtraq ID: 15720, December 5, 2005
GNU Mailman 2.1-2.1.5, 2.0-2.0.14	A remote Denial of Service vulnerability has been reported in 'Scrubber.py' due to a failure to handle exception conditions when Python fails to process an email file attachment that contains utf8 characters in its filename. **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	GNU Mailman Attachment Scrubber UTF8 Filename Remote Denial of Service CVE-2005-3573	Low	Secunia Advisory: SA17511, November 14, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:222, December 2, 2005**
Hewlett Packard Company HP-UX B.11.23, B.11.11, B.11.00	An unspecified vulnerability has been reported when IPSEC is running, which could let a remote malicious user obtain unauthorized access. Update information available at: http://www.securityfocus.com/advisories/9812 Currently we are not aware of any exploits for this vulnerability.	HP-UX Unspecified IPSec Unauthorized Remote Access CVE-2005-4090	Medium	HP Security Bulletin, HPSBUX02082, December 7, 2005
Hewlett Packard Company HP-UX B.11.23, B.11.22, B.11.11, B.11.04, B.11.00	A remote Denial of Service vulnerability has been reported in the Path MTU Discovery (PMTUD) functionality that is supported in the ICMP protocol. Patches available at: http://www1.itrc.hp.com/service/cki/docDisplay.do?docId= HPSBUX01137 Revision 2: The binary files of HPSBUX01164 will resolve the issue for the core TCP/IP in B.11.11, B.11.22, and B.11.23. The binary files of HPSBUX01164 will resolve NOT resolve the issue for IPSec. B.11.00 and B.11.04 are NOT vulnerable. The recommended workaround is to modify /etc/rc.config.d/nddconf and reboot. Rev 3: PHNE_33159 is available for B.11.11. Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-160.pdf Rev 4: PHNE_32606 is available for B.11.23. **Rev 6: IPSec revisions available.** Currently we are not aware of any exploits for this vulnerability.	HP-UX ICMP PMTUD Remote Denial of Service CVE-2005-1192	Low	Hewlett Packard Company Security Advisory, HPSBUX 01137, April 24, 2005 Hewlett Packard Company Security Advisory, HPSBUX 01137: SSRT5954 rev.1, May 25, 2005 Hewlett Packard Company Security Advisory, HPSBUX 01137: SSRT5954 rev.2, June 1, 2005 Avaya Security Bulletin, ASA-2005-160, July 15, 2005 HP Security Bulletin, HPSBUX0 1137 rev 4, July 19, 2005 **HP Security Bulletin, HPSBUX0 1137 rev 6, December 5, 2005**
IBM AIX 5.1-5.3	A vulnerability has been reported in the 'umountall' command due to an unspecified error with regards to the absolute path. The impact was not specified. Updates available at: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html Currently we are not aware of any exploits for this vulnerability.	IBM AIX UMOUNTALL Unspecified Absolute Path Security CVE-2005-4068	Not Specified	Secunia Advisory: SA17924, December 7, 2005
IPsec-Tools IPsec-Tools0.6-0.6.2, 0.5-0.5.2	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions when in 'AGGRESSIVE' mode. Upgrades available at: http://prdownloads.sourceforge.	IPsec-Tools ISAKMP IKE Remote Denial of Service	Low	Security Focus, Bugtraq ID: 15523, November 22, 2005 **Ubuntu Security Notice, USN-221-1, December**

	net/ipsec-tools/ipsec-tools-0.6.3.tar.bz2?download **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/i/ipsec-tools/** Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	CVE-2005-3732		**01, 2005**
libpng pnmtopng 2.38, 2.37.3-2.37.6	A buffer overflow vulnerability has been reported in 'Alphas_Of _Color' due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/png-mng/pnmtopng-2.39.tar.gz?download Debian: http://security.debian.org/pool/updates/main/n/netpbm-free/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	PNMToPNG Remote Buffer Overflow CVE-2005-3662	High	Security Focus, Bugtraq ID: 15427, November 15, 2005 Debian Security Advisory, DSA 904-1, November 21, 2005 Ubuntu Security Notice, USN-218-1, November 21, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:217, November 30, 2005** **SUSE Security Summary Report Announcement, SUSE-SR:2005:028, December 2, 2005**
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'Install Trigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for a remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/	Firefox Multiple Vulnerabilities CVE-2005-2260 CVE-2005-2261 CVE-2005-2262 CVE-2005-2263 CVE-2005-2264 CVE-2005-2265 CVE-2005-2267 CVE-2005-2269 CVE-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005

	Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ Debian: http://security.debian.org/pool/updates/main/m/mozilla/ Fedora: http://download.fedoralegacy.org/fedora/ HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBOV01229 HP: http://www.hp.com/products1/unix/		SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005 Debian Security Advisory, DSA 810-1, September 13, 2005 Fedora Legacy Update Advisory, FLSA:160202, September 14, 2005 HP Security Bulletin, HPSBOV01229, September 19, 2005 HP Security Bulletin, HPSBUX01230, October 3, 2005 Ubuntu Security Notice, USN-155-3, October 04, 2005 Sun(sm) Alert Notification Sun Alert ID: 101952, October 17, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**

	java/mozilla/index.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-locale-da/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101952-1 **SUSE:** **ftp://ftp.suse.com/pub/suse/** Exploits have been published.			
Multiple Vendors Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2; KDE kpdf 0.5, KOffice 1.4.2 ; PDFTOHTML DFTOHTML 0.36	Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code. Patches available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.01pl1.patch Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-840.html Currently we are not aware of any exploits for these vulnerabilities.	Xpdf Buffer Overflows CVE-2005-3191 CVE-2005-3192 CVE-2005-3193	High	iDefense Security Advisory, December 5, 2005 Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005 RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005

Multiple Vendors gnump3d 2.9-2.9.7; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Several vulnerabilities have been reported: a vulnerability was reported in the 'index.lok' lock file when indexing music files due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files; and a Directory Traversal vulnerability was reported when processing certain CGI parameters and cookie values due to an input validation error, which could let a remote malicious user obtain sensitive information. Update available at: http://savannah.gnu.org/download/gnump3d/ Debian: http://security.debian.org/pool/updates/main/g/gnump3d/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-16.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	GNU gnump3d Insecure Temporary File Creation & Directory Traversal CVE-2005-3349 CVE-2005-3355	Medium	Secunia Advisory: SA17647, November 18, 2005 Debian Security Advisory, DSA 901-1, November 19, 2005 Gentoo Linux Security Advisory, GLSA 200511-16, November 21, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
Multiple Vendors Linux Kernel Linux kernel 2.6- 2.6.14	A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPV6 Denial of Service CVE-2005-2973	Low	Secunia Advisory: SA17261, October 21, 2005 Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005 Security Focus, Bugtraq ID: 15156, October 31, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005**
Multiple Vendors phpMyAdmin 2.7 .0-beta1, 2.6.4 -rc1, pl3, pl1, 2.6.3 -pl1, 2.6.2 -rc1, 2.6.2, 2.6.1 pl3, 2.6.1 pl1, 2.6.1 -rc1, 2.6.1, 2.6.0pl3, 2.6.0pl2, 2.6.0pl1, 2.5.7pl1, 2.5.7, 2.5.6 -rc1, 2.5.5 pl1, 2.5.5 -rc2, 2.5.5 -rc1, 2.5.5, phpMyAdmin phpMyAdmin 2.5 .0-2.5.4, 2.4.0, 2.3.2, 2.3.1, 2.2-2.2.6, 2.1-2.1 .2, 2.0- 2.0.5	Cross-Site Scripting vulnerabilities have been reported in the 'HTTP_HOST' variable and certain scripts in the libraries directory due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.7.0.tar.gz There is no exploit code required.	PHPMyAdmin Multiple Cross-Site Scripting CVE-2005-3665	Medium	phpMyAdmin security announcement PMASA-2005-8, December 5, 2005
Multiple Vendors SuSE Linux Enterprise Server 9, Linux 9.3 x86_64; Linux kernel 2.6.11, 2.6.8, 2.6.5	A vulnerability has been reported in 'ptrace' 64-bit platforms, which could let a malicious user access kernel memory pages. SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva:**	Linux Kernel 64 Bit PTrace Kernel Memory Access CVE-2005-1763	Medium	SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:220, November 30, 2005**

	http://www.mandriva.com/security/advisories Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel XFRM Array Index Buffer Overflow CVE-2005-2456	High	Security Focus, 14477, August 5, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 200 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Linux Personal 10.0 OSS; Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported due to a race condition in 'do_coredump'. SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	Linux Kernel do_coredump Denial of Service CVE-2005-3527	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
Multiple Vendors Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0, SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server for S/390 9.0, Linux Enterprise Server 9; 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle malformed compressed files. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Null Pointer Dereference Denial of Service CVE-2005-2459	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**

Multiple Vendors
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
TouchTunes Rhapsody, TouchTunes Maestro;
SuSE UnitedLinux 1.0, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, 9.0 x86_64, 9.0, Linux Enterprise Server 9, 8, Linux Desktop 1.0;
RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, 2.1 IA64, 2.1, AS 4, AS 3, AS 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; GTK+ 2.8.6, 2.6.4, 2.4.14, 2.4.13, 2.4.10, 2.4.9, 2.4.1, 2.2.4, 2.2.3;
GNOME GdkPixbuf 0.22;
Gentoo Linux ; Ardour 0.99
	Multiple vulnerabilities have been reported: an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' due to the insufficient validation of the 'n_col' value before using to allocate memory, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when processing an XPM file that contains a large number of colors; and an integer overflow vulnerability was reported in '/gtk+/gdk-pixbuf/io-xpm.c' when performing calculations using the height, width, and colors of a XPM file, which could let a remote malicious user execute arbitrary code or cause a Denial of Service.
	Updates available at:
	ftp://ftp.gtk.org/pub/gtk/v2.8/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-810.html
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200511-14.xml
	SuSE:
	ftp://ftp.suse.com/pub/suse/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/g/gdk-pixbuf/
	Mandriva:
	http://www.mandriva.com/security/advisories
	Trustix:
	http://http.trustix.org/pub/trustix/
	Avaya:
	http://support.avaya.com/elmodocs2/security/ASA-2005-229.pdf
	Debian:
	http://security.debian.org/pool/updates/main/g/gtk+2.0/
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Debian:
	http://security.debian.org/pool/updates/main/g/gdk-pixbuf/
	Currently we are not aware of any exploits for these vulnerabilities.
		GTK+ GdkPixbuf XPM Image Rendering Library
		CVE-2005-2975
		CVE-2005-2976
		CVE-2005-3186
			High	Fedora Update Notifications FEDORA-2005-1085 & 1086, November 15, 2005
				RedHat Security Advisory, RHSA-2005:810-9, November 15, 2005
				Gentoo Linux Security Advisory GLSA 200511-14, November 16, 2005
				SUSE Security Announcement, SUSE-SA:2005:065, November 16, 2005
				Ubuntu Security Notice, USN-216-1, November 16, 2005
				Mandriva Linux Security Advisory, MDKSA-2005:214, November 18, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005
				Avaya Security Advisory, ASA-2005-229, November 21, 2005
				Debian Security Advisory, DSA 911-1, November 29, 2005
				SGI Security Advisory, 20051101-01-U, November 29, 2005
				Debian Security Advisory DSA 913-1, December 1, 2005

Multiple Vendors GNU gnump3d 2.9-2.9.5; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in GNUMP3d that could let remote malicious users conduct Cross-Site Scripting or traverse directories. Upgrade to version 2.9.6: http://savannah.gnu.org/download/gnump3d/gnump3d-2.9.6.tar.gz Debian:	GNUMP3d Cross-Site Scripting or Directory Traversal CVE-2005-3122 CVE-2005-3123	Medium	Security Focus Bugtraq IDs: 15226 & 15228, October 28, 2005 Debian Security Advisory DSA 877-1, October 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:025,

	http://security.debian.org/pool/updates/main/g/gnump3d/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Gentoo: http://security.gentoo.org/glsa/glsa-200511-05.xml There is no exploit code required; however, Proof of Concept exploits have been published.			November 4, 2005 Gentoo Linux Security Advisory, GLSA 200511-05, November 6, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
Multiple Vendors GNU gnump3d 2.9-2.9.5; Gentoo Linux	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.gnu.org/software/gnump3d/download.html#Download Gentoo: http://security.gentoo.org/glsa/glsa-200511-05.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	GNU gnump3d Unspecified Cross-Site Scripting CVE-2005-3425	Medium	Gentoo Linux Security Advisory GLSA 200511-05, November 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
Multiple Vendors Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Netfilter Memory Leak Denial of Service CVE-2005-0210	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 SUSE Security Announcement, SUSE-SA: 2005: 018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-21, August 9, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218 & 219, November 30, 2005**

Multiple Vendors Linux Kernel 2.6 up to & including 2.6.12-rc4	Several vulnerabilities have been reported: a vulnerability was reported in raw character devices (raw.c) because the wrong function is called before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space; and a vulnerability was reported in the 'pkt_ioctl' function in the 'pktcdvd' block device ioctl handler (pktcdvd.c) because the wrong function is called before passing an ioctl to the block device, which could let a malicious user execute arbitrary code. Update available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-420.html Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept Denial of Service exploit script has been published.	Multiple Vendor Linux Kernel pktcdvd & raw device Block Device CVE-2005-1264 CVE-2005-1589	High	Secunia Advisory, SA15392, May 17, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:110, July 1, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 Conectiva Linux Announcement, CLSA-2005:999, August 17, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005**
Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in the '/sys' file system due to a mismanagement of integer signedness, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code. SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntupool/main/l/linux-source-2.6.8.1/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS_Write_File Local Integer Overflow CVE-2005-0867	High	Security Focus, 13091, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005**
Multiple Vendors Linux Kernel 2.4.x, 2.6 prior to 2.6.11.11	A vulnerability has been reported in the Linux kernel in the Radionet Open Source Environment (ROSE) implementation in the 'rose_rt_ioctl()' function due to insufficient validation of a new routes' ndigis argument. The impact was not specified. Updates available at: http://linux.bkbits.net:8080/linux-2.4/cset@41e2cf515TpixcVQ8q8HvQvCv9E6zA Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/	Linux Kernel Radionet Open Source Environment (ROSE) ndigis Input Validation CVE-2005-3273	Not Specified	Security Tracker Alert, 1014115, June 7, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219, & 220, November 30, 2005**

	Mandriva: **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux Kernel 2.6 .10, 2.6, test-test11, 2.6.1-2.6.10, 2.6.10 rc2; RedHat Fedora Core2&3	An integer overflow vulnerability has been reported in the 'scsi_ioctl.c' kernel driver due to insufficient sanitization of the 'sg_scsi_ioctl' function, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SCSI IOCTL Integer Overflow CVE-2005-0180	High	Bugtraq, January 7, 2005 Fedora Update Notifications, FEDORA-2005-013 & 014, January 10, 2005 SUSE Security Announcement, SUSE-SA:2005:003, January 21, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:010, February 25, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6-test9-CVS, 2.6-test1-test11, 2.6, 2.6.1-2.6.11; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability was reported in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability was reported in the 'setsid()' function; and a vulnerability was reported in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-283.html http://rhn.redhat.com/errata/RHSA-2005-284.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-472.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf FedoraLegacy: http://download.fedoralegacy.org/redhat/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-420.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CVE-2005-0176 CVE-2005-0177 CVE-2005-0178 CVE-2005-0204	Medium	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 FedoraLegacy: FLSA:152532, June 4, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005**

Multiple Vendors Linux kernel 2.6.10-2.6.15	A Denial of Service vulnerability has been reported due to a memory leak in the kernel file lock lease code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.3.tar.bz2 SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	Linux Kernel File Lock Lease Local Denial of Service CVE-2005-3807	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2/EXT3 File Access Bypass CVE-2005-2801	Medium	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Ipt_recent' Remote Denial of Service CVE-2005-2872	Low	Security Focus, Bugtraq ID: 14791, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**
Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CVE-2005-2490 CVE-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005 RedHat Security Advisory, RHSA-2005:663-19,

	redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva: http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.			September 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ This issue has been addressed in Linux kernel 2.6.13-rc7. SUSE: ftp://ftp.SUSE.com/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva: http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CVE-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005 Security Focus, Bugtraq ID 14609, August 25, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .3, 2.4-2.4.32	A Denial of Service vulnerability has been reported in 'IP_VS_CONN_FLUSH' due to a NULL pointer dereference. Kernel versions 2.6.13 and 2.4.32-pre2 are not affected by this issue. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva: http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Denial of Service CVE-2005-3274	Low	Security Focus, Bugtraq ID: 15528, November 22, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12, 2.4-2.4.31	A remote Denial of Service vulnerability has been reported due to a design error in the kernel. The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue. Ubuntu: http://security.ubuntu.com/ubuntu/pool/	Linux Kernel Remote Denial of Service CVE-2005-3275	Low	Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005**

	main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6-2.6.13.1	A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function. Fixed version (2.6.13.2), available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel routing_ioctl() Denial of Service CVE-2005-3044	Low	Security Tracker Alert ID: 1014944, September 21, 2005 Ubuntu Security Notice, USN-187-1, September 25, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219, 220, November 30, 2005** **SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-808.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Linux Kernel Denial of Service & Information Disclosure CVE-2005-3119 CVE-2005-3180 CVE-2005-3181	Medium	Secunia Advisory: SA17114, October 12, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005** **SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling asynchronous USB access via usbdevio; and a Denial of Service vulnerability was reported in the 'ipt_recent.c' netfilter module due to an error in jiffies comparison. RedHat:	Linux Kernel USB Subsystem Denials of Service CVE-2005-2873 CVE-2005-3055	Low	Secunia Advisory: SA16969, September 27, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 Ubuntu Security Notice,

	http://rhn.redhat.com/ errata/RHSA-2005-514.html Ubuntu: http://security.ubuntu. com/ubuntu/pool/ main/l/ **Mandriva: http://www.mandriva. com/security/ advisories** **SUSE: ftp://ftp.suse.com /pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.			USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005** **SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_ mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of a non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on a SMP system that is operating under a heavy load. Ubuntu: http://security.ubuntu. com/ubuntu/pool/ main/l/ Trustix: http://http.trustix.org/ pub/trustix/updates/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-808.html **Mandriva: http://www.mandriva. com/security/ advisories** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Denials of Service CVE-2005-3053 CVE-2005-3106 CVE-2005-3107 CVE-2005-3108 CVE-2005-3109 CVE-2005-3110	Low	Ubuntu Security Notice, USN-199-1, October 10, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005 RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005 **Mandriva Linux Security Advisories, MDKSA-2005: 219 & 220, November 30, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14, 2.5.0- 2.5.69, 2.4-2.4.32, 2.3, 2.3.x, 2.3.99, pre1-pre7, 2.2-2.2.27, 2.1, 2.1 .x, 2.1.89, 2.0.28-2.0.39	A vulnerability has been reported due to the way console keyboard mapping is handled, which could let a malicious user modify the console keymap to include scripted macro commands. **Mandriva: http://www.mandriva. com/security/ advisories** There is no exploit code required; however, a Proof of Concept exploit has been published.	Linux Kernel Console Keymap Arbitrary Command Injection CVE-2005-3257	Medium	Security Focus, Bugtraq ID: 15122, October 17, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005**

Multiple Vendors
 	
Linux kernel 2.6-2.6.14;
SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS;
RedHat Fedora Core4
	A Denial of Service vulnerability has been reported in 'ptrace.c' when 'CLONE_THREAD' is used due to a missing check of the thread's group ID when trying to determine whether the process is attempting to attach to itself.
	
	Upgrades available at:
	http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.2.tar.bz2
	
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/
	
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel PTrace 'CLONE_THREAD' Denial of Service
		
		CVE-2005-3783
			Low	Secunia Advisory: SA17761, November 29, 2005
				
				Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
				
				SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005

Multiple Vendors
 	
Linux kernel 2.6-2.6.15;
SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS;
RedHat Fedora Core4
	A Denial of Service vulnerability has been reported because processes are improperly auto-reaped when they are being ptraced.
	
	Patches available at:
	http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.15-rc3.bz2
	
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/
	
	SUSE:
	ftp://ftp.SUSE.com/pub/SUSE
	
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel PTraced Denial of Service
		
		CVE-2005-3784
			Low	Security Focus, Bugtraq ID: 15625, November 29, 2005
				
				Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
				
				SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005

Multiple Vendors Linux kernel 2.6-2.6.12 .1	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling key rings; and a Denial of Service vulnerability was reported in the 'KEYCTL_JOIN_SESSION_KEYRING' operation due to an error when attempting to join a key management session. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.13-rc6-git 1.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	Linux Kernel Management Denials of Service CVE-2005-2098 CVE-2005-2099	Low	Secunia Advisory: SA16355, August 9, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:220, November 30, 2005**
Multiple Vendors RedHat Fedora Core3; Linux kernel 2.6.10-2.6.13	A vulnerability has been reported because a world writable file is created in 'SYSFS' which could let a malicious user obtain sensitive information. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.13.4.tar.bz2 Fedora:	Linux Kernel World Writable SYSFS Information Disclosure CVE-2005-3179	Medium	Security Focus, Bugtraq ID: 15154, October 20, 2005 Fedora Update Notification FEDORA-2005-1007, October 20, 2005 **Mandriva Linux Security Advisory,**

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.			**MDKSA-2005:220, November 30, 2005**
Multiple Vendors SpamAssassin 3.0.4; RedHat Fedora Core3	A vulnerability has been reported due to a failure to handle exceptional conditions, which could let a remote malicious user bypass spam detection. SpamAssassin: http://spamassassin.apache.org/downloads.cgi?update=200509141634 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	SpamAssassin Spam Detection Bypass CVE-2005-3351	Medium	Fedora Update Notification, FEDORA-2005-1065, November 9, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0064, November 22, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:221, December 2, 2005**
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Personal 10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32	A Denial of Service vulnerability has been reported in FlowLable. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.6/linux-2.6.14.tar.bz2 SUSE: ftp://ftp.suse.com/pub/suse/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPv6 FlowLable Denial of Service CVE-2005-3806	Low	Security Focus, Bugtraq ID: 15729, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0 OSS; Linux kernel 2.6.10 -2.6.14	A Denial of Service vulnerability has been reported due to a race condition error in the handling of POSIX timer cleanup routines. Linux kernel versions subsequent to 2.6.14 are not vulnerable to this issue. SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for this vulnerability.	Linux Kernel POSIX Timer Cleanup Handling Local Denial of Service CVE-2005-3805	Low	SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
Multiple Vendors Turbolinux Server 10.0, 8.0, Desktop 10.0, Turbolinux Home Appliance Server 1.0 Workgroup Edition, Hosting Edition; Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0; Sun Solaris 10.0 _x86, 10.0, 9.0 _x86 Update 2, 9.0 _x86, 9.0, Sun SEAM 1.0-1.0.2; SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when a malicious user submits a specially crafted TCP connection that causes the Key Distribution Center (KDC) to attempt to free random memory; a buffer overflow vulnerability was reported in KDC due to a boundary error when a specially crafted TCP or UDP request is submitted, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in 'krb/recvauth.c' which could let a remote malicious user execute arbitrary code. MIT: http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt.asc	Kerberos V5 Multiple Vulnerabilities CVE-2005-1174 CVE-2005-1175 CVE-2005-1689	High	MIT krb5 Security Advisory, 2005-002, July 12, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 Sun(sm) Alert Notification, 101809, July 12, 2005 Fedora Update Notifications, FEDORA-2005-552 & 553, July 12, 2005 SUSE Security Summary Report,

x86_64, 9.3; RedHat Fedora Core3 & 4, Advanced Workstation for the Itanium Processor 2.1; MIT Kerberos 5 5.0 -1.4.1 & prior; Gentoo Linux	Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-567.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1 SuSE: http://www.novell.com/linux/security/advisories.html Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://www.sgi.com/support/security/ Debian: http://www.debian.org/security/2005/dsa-757 Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000993 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101810-1 RedHat: http://rhn.redhat.com/errata/RHSA-2005-562.html **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/k/krb4/** Currently we are not aware of any exploits for these vulnerabilities.			SUSE-SR:2005:017, July 13, 2005 Turbolinux Security Advisory TLSA-2005-78, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005: 119, July 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005- 0036, July, 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 Debian Security Advisory, DSA-757-1, July 17, 2005 US-CERT VU#885830 US-CERT VU#623332 US-CERT VU#259798 Conectiva Linux Advisory, CLSA-2005 :993, August 8, 2005 Sun(sm) Alert Notification Sun Alert ID: 101810, August 29, 2005 RedHat Security Advisory, RHSA-2005:562-15, Updated October 5, 2005 **Ubuntu Security Notice, USN-224-1, December 06, 2005**
Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6.8, rc1&rc2	A remote Denial of Service vulnerability has been reported when handling UDP packets received by SNMPD due to a NULL pointer dereference. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SNMP Handler Remote Denial of Service CVE-2005-2548	Low	Ubuntu Security Notice, USN-169-1, August 19, 20 **Mandriva Linux Security Advisory, MDKSA-2005:219, November 30, 2005**

Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.8	A Denial of Service vulnerability has been reported due to a resource leak when handling POSIX timers in the 'exec()' function. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Resource Leak Denial of Service CVE-2005-3271	Low	Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218 & 219, November 30, 2005** **SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, rc2, 2.6.8, rc1	A remote Denial of Service vulnerability has been reported in the kernel driver for compressed ISO file systems when attempting to mount a malicious compressed ISO image. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ISO File System Remote Denial of Service CVE-2005-2457	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0; SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9; Linux kernel 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Invalid Memory Access Denial of Service CVE-2005-2458	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005**
Multiple Vendors Ubuntu Linux 5.0 4, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.13	A Denial of Service vulnerability has been reported in the '/proc/scsi/sg/devices' file due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.**	Linux Kernel SCSI ProcFS Denial of Service CVE-2005-2800	Low	Security Focus, Bugtraq ID: 14790, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 **Mandriva Linux Security Advisories,**

	com/security/advisories A Proof of Concept exploit has been published.			**MDKSA-2005:218, 219, & 220, November 30, 2005**

Multiple Vendors
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
IBM HTTP Server 2.0.47.1, 2.0.47, 2.0.42.2, 2.0.42.1, 2.0.42;
Apache 2.0.28-2.0.54, 2.0 a9, 2.0
	A remote Denial of Service vulnerability has been reported in 'worker.c' due to a memory leak.
	Apache:
	http://www.apache.org/dist/httpd/Announcement2.0.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/a/apache2/
	IBM:
	http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24010709
	There is no exploit code required.
		Apache MPM 'Worker.C' Remote Denial of Service
		CVE-2005-2970
			Low	Security Focus, Bugtraq ID: 15762, December 7, 2005
				Ubuntu Security Notice, USN-225-1, December 06, 2005

Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Netpbm 10.0, 9.20 -9.25; libpng pnmtopng 2.38, 2.37.3-2.37.6; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A buffer overflow vulnerability has been reported due to insufficient bounds checking of user-supplied data prior to copying it to an insufficiently sized memory buffer, which could let a remote malicious user execute arbitrary code. libpng: http://prdownloads.sourceforge.net/png-mng/pnmtopng-2.39.tar.gz?download Debian: http://security.debian.org/pool/updates/main/n/netpbm-free/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	NetPBM PNMToPNG Remote Buffer Overflow CVE-2005-3632	High	Debian Security Advisory DSA 904-1, November 21, 2005 Ubuntu Security Notice, USN-218-1 November 21, 2005 **Mandriva Linux Security Advisory, MDKSA-2005:217, November 30, 2005** **SUSE Security Summary Report Announcement, SUSE-SR:2005:028, December 2, 2005**
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Linux kernel 2.6-2.6.12 .3	An information disclosure vulnerability has been reported in 'SYS_GET_THREAD_AREA,' which could let a malicious user obtain sensitive information. Kernel versions 2.6.12.4 and 2.6.13 are not affected by this issue. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Information Disclosure CVE-2005-3276	Medium	Ubuntu Security Notice, USN-219-1, November 22, 2005 **Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005**

Multiple Vendors Webmin 0.88 -1.230, 0.85, 0.76-0.80, 0.51, 0.42, 0.41, 0.31, 0.22, 0.21, 0.8.5 Red Hat, 0.8.4, 0.8.3, 0.1-0.7; Usermin 1.160, 1.150, 1.140, 1.130, 1.120, 1.110, 1.0, 0.9-0.99, 0.4-0.8; Larry Wall Perl 5.8.3-5.8.7, 5.8.1, 5.8 .0-88.3, 5.8, 5.6.1, 5.6, 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03	A format string vulnerability has been reported in 'Perl_sv_ vcatpvfnl' due to a failure to properly handle format specifiers in formatted printing functions, which could let a remote malicious user cause a Denial of Service. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates** **OpenPKG:** **http://www.openpkg.org/security.html** **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/perl/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200512-01.xml** **http://security.gentoo.org/glsa/glsa-200512-02.xml** An exploit has been published.	Perl 'miniserv.pl' script Format String CVE-2005-3912 **CVE-2005-3962**	Low	Security Focus, Bugtraq ID: 15629, November 29, 2005 **Fedora Update Notifications, FEDORA-2005-1113, 1116, & 1117, December 1 & 2, 2005** **OpenPKG Security Advisory, OpenPKG-SA-2005.025, December 3, 2005** **Mandriva Linux Security Advisory, MDKSA-2005:223, December 2, 2005** **Ubuntu Security Notice, USN-222-1 December 02, 2005, December 2, 2005** **Gentoo Linux Security Advisory, GLSA 200512-01 & 200512-02, December 7, 2005** **US-CERT VU#948385**
Opera Software Opera Web Browser 8.5, 8.0-8.0 2	A vulnerability has been reported due to insufficient sanitization of user-supplied data passed through a URI, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.opera.com/download/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Opera Web Browser Arbitrary Command Execution CVE-2005-3750	High	Secunia Advisory: SA16907, November 22, 2005 **SUSE Security Summary Report Announcement, SUSE-SR:2005:028, December 2, 2005**
phpMyAdmin phpMyAdmin 2.6 .0-2.6.3, 2.5 .0-2.5.7, 2.4 .0, 2.3.2, 2.3.1, 2.2 -2.2.6, 2.1-2.1 .2, 2.0-2.0.5	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported in 'libraries/auth/ cookie.auth.lib.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability has been reported in 'error.php' due to insufficient sanitization of the 'error' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=23067 Debian: http://security.debian.org/pool/updates/main/p/phpmyadmin/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPMyAdmin Cross-Site Scripting CVE-2005-2869	Medium	Secunia Advisory: SA16605, August 29, 2005 Debian Security Advisory, DSA 880-1, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 SUSE Security Announcement, SUSE-SA:2005:066, November 18, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
phpMyAdmin phpMyAdmin 2.7 .0-beta1, 2.7	A vulnerability has been reported in the register_globals emulation layer in 'grab_ globals.php' because the 'import_blacklist' variable is not properly protected, which could let a remote malicious user execute arbitrary HTML and script code and include arbitrary files. Upgrades available at: http://prdownloads.sourceforge.	PHPMyAdmin 'Import_Blacklist' Variable Overwrite CVE-2005-4079	Medium	Secunia Advisory: SA17925, December 7, 2005

	net/phpmyadmin/phpMyAdmin-2.7.0-pl1.tar .gz There is no exploit code required.			
phpMyAdmin phpMyAdmin 2.x	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of certain configuration parameters, which could let a remote malicious user include arbitrary files; and a Cross-Site Scripting vulnerability was reported in 'left.php,' 'queryframe.php,' and 'server_databases.php' due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.6.4-pl3.tar .gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-21.xml Debian: http://security.debian.org/pool/updates/main/p/phpmyadmin/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required; however, a Proof of Concept exploit has been published.	phpMyAdmin Local File Inclusion & Cross-Site Scripting CVE-2005-3300 CVE-2005-3301	Medium	Secunia Advisory: SA17289, October 24, 2005 Gentoo Linux Security Advisory, GLSA 200510-21, October 25, 2005 Debian Security Advisory, DSA 880-1, November 2, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 SUSE Security Announcement, SUSE-SA:2005:066, November 18, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
SAMEDIA LandShop 0.6.3	SQL injection vulnerabilities have been reported in 'ls.php' due to insufficient sanitization of the 'start,' 'search_order,' 'search_type,' 'search_area,' and 'keyword' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploit scripts have been published.	SAMEDIA Landshop Multiple SQL Injection CVE-2005-4018	Medium	Secunia Advisory: SA17843, December 5, 2005
Sun Microsystems, Inc. Java System Messaging Server 6 2005Q1	A vulnerability has been reported in the Communications Services Delegated Administrator due to an unspecified error, which could let a remote malicious user obtain sensitive information. Patch information available at: http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102068-1 Currently we are not aware of any exploits for this vulnerability.	Sun Communications Services Delegated Administrator Default Password Disclosure CVE-2005-4045	Medium	Sun(sm) Alert Notification, Sun Alert ID: 102068, December 5, 2005
SuSE SuSE Linux Professional 9.0, x86_64, Linux Personal 9.0, x86_64	A remote Denial of Service vulnerability has been reported in the squid proxy when handling specially crafted HTTPs data. **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.	SUSE Linux Squid Proxy SSL Handling Remote Denial of Service CVE-2005-3322	Low	SUSE Security Summary Report, Announcement ID: SUSE-SR:2005:024, October 21, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
Sylpheed Sylpheed 2.0-2.0.3, 1.0.0-1.0.5	A buffer overflow vulnerability has been reported in 'ldif.c' due to a boundary error in the 'ldif_get_line()' function when importing a LDIF file into the address book, which could let a remote malicious user obtain unauthorized access. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.6.tar.gz Fedora:	Sylpheed LDIF Import Buffer Overflow CVE-2005-3354	Medium	Bugtraq ID: 15363, November 9, 2005 Fedora Update Notification, FEDORA-2005-1063, November 9, 2005 Gentoo Linux Security Advisory, GLSA 200511-13, November 15, 2005

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-13.xml Debian: http://security.debian.org/pool/updates/main/s/sylpheed/ Debian: http://security.debian.org/pool/updates/main/s/sylpheed-claws/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for this vulnerability.			Debian Security Advisory, DSA 906-1, November 22, 2005 Debian Security Advisory, DSA 908-1, November 23, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
The Open Group Open Motif 2.2.3	Two buffer overflow vulnerabilities have been reported in libUil (User Interface Language): a buffer overflow vulnerability was reported in 'diag_issue_diagnostic()' due to the use of the vsprintf() libc procedure, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in 'open_source_file()' due to the use of the strcpy() libc procedure, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Open Motif libUil Buffer Overflows CVE-2005-3964	High	Security Focus, Bugtraq ID: 15678, December 2, 2005
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/u/uw-imap/ Gentoo: http://security.gentoo.org/glsa/glsa-200510-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/ security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-848.html**	UW-imapd Denial of Service and Arbitrary Code Execution CVE-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005 Debian Security Advisory, DSA 861-1, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005 US-CERT VU#933601 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005 Slackware Security Advisory, SSA:2005-310-06, November 7, 2005 Conectiva Linux Announcement, CLSA-2005:1046, November 21, 2005 **RedHat Security Advisory, RHSA-2005:848-6 & 850-5, December 6, 2005**

	http://rhn.redhat.com/errata/RHSA-2005-850.html Currently we are not aware of any exploits for this vulnerability.	

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
1-Script 1-Search 1.8	A Cross-Site Scripting vulnerability has been reported in '1search.cgi' due to insufficient sanitization of the 'q' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	1-Script 1-Search Cross-Site Scripting CVE-2005-4091	Medium	Security Focus, Bugtraq ID: 15712, December 5, 2005
88Script Event Calendar 2.0	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'm' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	88Scripts Event Calendar Index.PHP SQL Injection CVE-2005-3933	Medium	Security Focus, Bugtraq ID: 15658, November 30, 2005
Alisveristr E-commerce	SQL injection vulnerabilities have been reported in the commerce login due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	Alisveristr E-Multiple SQL Injection CVE-2005-4081	Medium	Security Focus, Bugtraq ID: 15699, December 3, 2005
All Time Flash Dreamer FileLister 0.51	A Cross-Site Scripting vulnerability has been reported in 'definesearch.jsp' due to insufficient sanitization of the 'searchwhat' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	FileLister Cross-SIte Scripting CVE-2005-4040	Medium	Security Focus, Bugtraq ID: 15706, December 5, 2005

Apple QuickTime Player 7.0.3, iTunes 6.0.1	A heap-based overflow vulnerability has been reported which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Quicktime/ iTunes Heap Overflow CVE-2005-4092	High	Security Focus, Bugtraq ID: 15732, December 6, 2005
Atlantis Knowledge Base Atlantis Knowledge Base 3.0	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'searchStr' parameter when performing a search before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Atlantis Knowledge Base Software SQL Injection CVE-2005-3881	Medium	Security Focus Bugtraq ID: 15654, November 30, 2005
Atlassian Software Systems Atlassian Confluence 2.0.1 build 321	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'searchQuery' parameter when performing a search before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Atlassian Confluence Cross-Site Scripting CVE-2005-3994	Medium	Security Focus, Bugtraq ID: 15688, December 2, 2005
Avaya Avaya TN2602AP IP Media Resource 320 vintage 3-vintage7	A remote Denial of Service vulnerability has been reported due to an unspecified error. Upgrades available at: http://support.avaya.com/japple/css/japple?temp.documentID=236667&temp .productID=136527&temp.releaseID=228560&temp.bucketID=108025&PAGE=Docu ment#TN2602 Currently we are not aware of any exploits for this vulnerability.	Avaya TN2602AP IP Media Resource 320 Remote Denial of Service CVE-2005-3989	Low	Avaya Security Advisory, ASA-2005-231, November 30, 2005
Check Point Software SecureClient NG with Application Intelligence R56, SecureClient NG FP1, 4.1, 4.0	A vulnerability has been reported due to a failure to securely implement remote administrator-provided policies, which could let a remote malicious user bypass security policies. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Check Point VPN-1 SecureClient Policy Bypass CVE-2005-4093	Medium	Security Focus, Bugtraq ID: 15757, December 7, 2005

Cisco Systems Firewall Services Module (FWSM) 1.x, 2.x, IOS 12.x, IOS R12.x, PIX 4.x, 5.x, 6.x, 7.x, Cisco SAN-OS 1.x (MDS 9000 Switches), 2.x (MDS 9000 Switches), VPN 3000 Concentrator	A remote Denial of Service vulnerability has been reported due to errors in the processing of IKEv1 Phase 1 protocol exchange messages. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec.shtml Rev 1.5: Updated Cisco IOS Products table. **Rev 1.6: Updated Additional Details for Cisco IOS section. Updated Cisco IOS section.** Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	Cisco IPSec IKE Traffic Remote Denial of Service CVE-2005-3669	Low	Cisco Security Advisory, Document ID: 68158, November 14, 2005 Cisco Security Advisory, Document ID: 68158, Rev 1.5, November 29, 2005 **Cisco Security Advisory, Document ID: 68158, Rev 1.6, December 6, 2005**
Cisco Systems IOS 12.0 (2a)	An HTTP injection vulnerability has been reported in the '/level/14/exec/buffers/assigned/' and '/level/14/exec/buffers/all' scripts, which could let a remote malicious user execute arbitrary HTML and script code. **Workaround information available at: http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml** There is no exploit code required; however, a Proof of Concept exploit has been published.	Cisco IOS HTTP Service HTML Injection CVE-2005-3921	Medium	Security Focus, Bugtraq ID: 15602, November 28, 2005 **Cisco Security Advisory, cisco-sa-20051201-http, December 1, 2005**
DoceboLMS DoceboLMS 2.0.4	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in the 'connector.php' script due to insufficient validation of the 'Type' parameter, which could let a remote malicious user obtain sensitive information; and an input validation vulnerability was reported in the file upload handling due to insufficient verification of the file extension of valid images, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	DoceboLMS Directory Traversal & File Upload CVE-2005-4094 CVE-2005-4095	High	Security Tracker Alert ID: 1015308, December 5, 2005
Dotclear Dotclear 1.2.2, 1.2.1	An SQL injection vulnerability has been reported in 'session.php' due to insufficient sanitization of '/inc/session.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://www.dotclear.net/download/dotclear-1.2.3.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	DotClear SQL Injection CVE-2005-3963	Medium	Zone-H Research Team Security Advisory, ZRCSA-200504, November 30, 2005

Drupal Drupal 4.6-4.6.3, 4.5-4.5.5	Multiple vulnerabilities have been reported: an input validation vulnerability was reported when filtering HTML code, which could let a remote malicious user inject arbitrary JavaScript code; an input validation vulnerability was reported due to an error in the attachment handling, which could let a remote malicious user upload a malicious image and inject arbitrary HTTP headers; and a vulnerability was reported in the 'access user profile' permission can a remote malicious user can bypass it. Upgrades available at: http://drupal.org/files/projects/drupal-4.5.6.tar.gz There is no exploit code required.	Drupal Multiple Vulnerabilities CVE-2005-3973 CVE-2005-3974 CVE-2005-3975	Medium	Secunia Advisory: SA17824, December 1, 2005
DUware DUportal Pro 3.4.3	A Cross-Site Scripting vulnerability has been reported in 'password.asp' due to insufficient sanitization of the 'result' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	DuWare DuPortalPro Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 15731, December 6, 2005
e107.org e107 website system 0.617-0.6172, 0.616, 0.603, 0.555 Beta, 0.554, 0.545, 0.6 10-0.6 15a	Several vulnerabilities have been reported: a vulnerability was reported due to the way an unverified user supplied argument is used to redirect a user after the user has submitted a file download rating, which could let a remote malicious user redirected users to an untrusted (fake) site; and a vulnerability was reported due to the way users are prevented from submitting multiple ratings for a file download, which could let a remote malicious user bypass security restrictions and submit multiple votes. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	e107 Website System Redirection & Voting Manipulation CVE-2005-4051 CVE-2005-4052	Medium	Secunia Advisory: SA17890, December 5, 2005
efiction Project efiction 2.0, 1.1, 1.0	Multiple vulnerabilities have been reported: a vulnerability was reported in 'titles.php' due to insufficient sanitization of the 'let' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in the 'Manage Images' functionality due to an	eFiction Input Validation	Medium	Secunia Advisory: SA17777, November 28, 2005 **Security Focus, Bugtraq ID: 15568, December 6, 2005**

	input validation error, which could let a remote malicious user upload valid images with an arbitrary file extension inside the web root; and a vulnerability was reported in 'phpinfo.php' because a remote malicious user can obtain sensitive information. **The vendor has released a fix to resolve these issues.** There is no exploit code required; however, Proof of Concept exploits and an exploit script have been published.			
Extreme Corporate Extreme Search Corporate Edition 6.0	A Cross-Site Scripting vulnerability has been reported in 'extremesearch.php' due to insufficient sanitization of the 'search' before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Extreme Corporate Cross-Site Scripting CVE-2005-3972	Medium	Security Focus, Bugtraq ID: 15675, December 1, 2005
FaqRing FaqRing 3.0	An SQL injection vulnerability has been reported in 'answer.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	FAQRing SQL Injection CVE-2005-3882	Medium	Secunia Advisory: SA17811, November 30, 2005
FastJar FastJar 0.93	A Directory Traversal vulnerability has been reported due to an input validation error when extracting compressed '.jar' archives, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	FastJar Archive Extraction Directory Traversal CVE-2005-3990	Medium	Secunia Advisory: SA17839, December 1, 2005
FFmpeg FFmpeg 0.4.9 -pre1, 0.4.6-0.4.8, FFmpeg CVS	A buffer overflow vulnerability has been reported in the 'avcodec_default_get_buffer()' function of 'utils.c' in libavcodec due to a boundary error, which could let a remote malicious user execute arbitrary code. Patches available at: http://www1.mplayerhq.hu/cgi-bin/cvsweb.cgi/ffmpeg/libavcodec/utils.c.diff?cvsroot=FFMpeg&r2=1.162&r1=1.161&f=u Currently we are not aware of any exploits for this vulnerability.	FFmpeg Remote Buffer Overflow CVE-2005-4048	High	Secunia Advisory: SA17892, December 6, 2005

Globalissa phpYellowTM Pro 5.33, phpYellowTM Lite 5.33	SQL injection vulnerabilities have been reported in 'search_result.php' due to insufficient sanitization of the 'haystack' parameter and in 'print_me.php' due to insufficient sanitization of the 'ckey' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	PHPYellowTM Multiple SQL Injection CVE-2005-4001	Medium	Security Focus, Bugtraq ID: 15700, December 3, 2005
Hobosworld HobSR	SQL injection vulnerabilities have been reported in 'view.php' due to insufficient sanitization of the 'arrange' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Hobosworld HobSR Multiple SQL Injection CVE-2005-4043	Medium	Secunia Advisory: SA17884, December 5, 2005
Horde IMP 4.0-4.0.4, 3.2-3.2.5, 3.1.2, 3.1, 3.0, 2.3, 2.2-2.2.8, 2.0	An HTML injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Horde IMP Email Attachments HTML Injection CVE-2005-4080	Medium	Security Tracker Alert ID: 1015315, December 6, 2005
Horde Project Horde 2.2-2.2.8	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified parameters before returning to the user in error messages, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/horde/horde-2.2.9.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200511-20.xml **Debian:** **http://security.debian.org/pool/updates/main/h/horde2/** There is no exploit code required.	Horde Error Message Cross-Site Scripting CVE-2005-3570	Medium	Secunia Advisory: SA17468, November 14, 2005 Gentoo Linux Security Advisory, GLSA 200511-20, November 22, 2005 **Debian Security Advisory DSA 914-1, December 1, 2005**

Inkscape Inkscape 0.41	A vulnerability has been reported in 'ps2epsi.sh' due to the insecure creation of a temporary file, which could let a malicious user create/overwrite arbitrary files. Upgrade available at: http://citkit.dl.sourceforge.net/sourceforge/inkscape/inkscape-0.42.ta r.gz **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/i/inkscape/** **Debian:** **http://security.debian.org/pool/updates/main/i/inkscape/** There is no exploit code required.	Inkscape 'ps2epsi.sh' Insecure Temporary File CVE-2005-3885	Medium	Security Focus 14522, August 9, 2005 **Ubuntu Security Notice, USN-223-1, December 05, 2005** **Debian Security Advisory, DSA 916-1, December 7, 2005**
Instant Photo Gallery Instant Photo Gallery 1.0	SQL injection vulnerabilities have been reported in 'portfolio.php' due to insufficient sanitization of the 'cat_id' parameter and in 'content.php' due to insufficient sanitization of the 'cid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Instant Photo Gallery SQL Injection CVE-2005-3986	Medium	Secunia Advisory: SA17841, December 1, 2005
Java Search Engine Java Search Engine 0.9.34	A Cross-Site Scripting vulnerability has been reported in 'search.jsp' due to insufficient of the 'q' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.	Java Search Engine Cross-Site Scripting CVE-2005-3966	Medium	Security Focus, Bugtraq ID: 15687, December 2, 2005
Mambo Mambo Site Server 4.0.14, 4.0.12 RC1-RC3, BETA & BETA 2, 4.0.10-4.0.12, 4.0	A remote file include vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary remote PHP code. The vendor has released a patch addressing this issue. Users are advised to contact the vendor for more information on obtaining the appropriate patch. An exploit script has been published. **Reports indicate that a bot is propagating in the wild by exploiting this vulnerability.**	Mambo Open Source Remote File Include CVE-2005-3738	High	Security Focus, Bugtraq ID: 15461, November 16, 2005 Security Focus, Bugtraq ID: 15461, November 21, 2005 Security Focus, Bugtraq ID: 15461, November 24, 2005 **Security Focus, Bugtraq ID: 15461, December 5, 2005**
MediaWiki MediaWiki 1.5.0-1.5.2, beta1-beta3,	A vulnerability has been reported in the user language option due to insufficient verification of user-supplied input before used in an 'eval()'	MediaWiki User Language Remote Code Execution	High	Security Focus, Bugtraq ID: 15703, December 5, 2005 US-CERT VU#392156

alpha1 & alpha2,	call, which could let a remote malicious user execute arbitrary PHP code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.5.3.tar.gz There is no exploit code required.	CVE-2005-4067		
Mr. CGI Guy Warm Links 1.0, Hot Links SQL 3.1, Hot Links Pro 3.0, Amazon Search Directory 1.0	A Cross-Site Scripting vulnerability has been reported in 'search.cgi' due to insufficient sanitization of the 'search' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Mr CGI Guy Multiple Software Search.CGI Cross-Site Scripting CVE-2005-4041 CVE-2005-4042 CVE-2005-4044	Medium	Security Focus, Bugtraq ID: 15708, December 5, 2005
Multiple Vendors Insyde BIOS V190; AWARD BIOS Modular 4.50 pg	A vulnerability has been reported due to a failure to clear the keyboard buffer after reading the BIOS password during the system startup process, which could let a remote malicious user obtain the BIOS password. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor BIOS Password Persistence Weakness	Medium	Security Focus, Bugtraq ID: 15751, December 6, 2005
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64; Inkscape 0.42, 0.41	A buffer overflow vulnerability has been reported in the SVG importer due to a boundary error, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/inkscape/ Gentoo: http://security.gentoo.org/glsa/glsa-200511-22.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Debian:** **http://security.debian.org/pool/updates/main/i/inkscape/** A Proof of Concept Denial of Service exploit has been published.	Inkscape SVG Image Buffer Overflow CVE-2005-3737	High	Ubuntu Security Notice, USN-217-1, November 21, 2005 Gentoo Linux Security Advisory, GLSA 200511-22, November 28, 2005 **SUSE Security Summary Report Announcement, SUSE-SR:2005:028, December 2, 2005** **Debian Security Advisory, DSA 916-1, December 7, 2005**
Multiple Vendors University of Kansas Lynx 2.8.5 & prior	A vulnerability has been reported in the 'lynxcgi:' URI handler, which could let a remote malicious user execute arbitrary commands. Upgrades available at: http://lynx.isc.org/current/lynx2.8.6dev.15.tar.gz RedHat: http://rhn.redhat.com/errata/RHSA-2005-839.html	Lynx URI Handlers Arbitrary Command Execution CVE-2005-2929	High	Security Tracker Alert ID: 1015195, November 11, 2005 RedHat Security Advisory, RHSA-2005:839-3, November 11, 2005 Mandriva Linux Security Advisory, MDKSA-2005:211, November 12, 2005 Gentoo Linux Security Advisory, GLSA

	Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200511-09.xml Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **OpenPKG: http://www.openpkg.org/** There is no exploit code required.			200511-09, November 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005 SGI Security Advisory, 20051101-01-U, November 29, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.026, December 3, 2005**
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLE pre122300, -STABLE pre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE -p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLE pre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE,	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability was reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability was reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail /security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/ nph-reg3rdpty1.pl/product=05529& platform=osx&method=sa/SecUpd 2005-003Pan.dmg Debian: http://security.debian.org/pool/ updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch _1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall:	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CVE-2005-0468 CVE-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005

-RELENG, 4.6 -RELEASE -p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRE RELEASE, 4.8, 4.9 -RELENG, 4.9 -PRE RELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRE RELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386; SGI IRIX 6.5.24-6.5.27	http://www.openwall.com/Owl/ CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/ document.do?assetkey= 1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/ en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/		SGI Security Advisory, 20050405-01-P, May 26, 2005 Debian Security Advisory, DSA 731-1, June 2, 2005 Conectiva Security Advisory, CLSA-2005:962, June 6, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Avaya Security Advisory, ASA-2005-132, June 14, 2005 Fedora Legacy Update Advisory, FLSA:152583, July 11, 2005 Slackware Security Advisory, SSA:2005-210-01, August 1, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 Security Focus, Bugtraq ID: 12919, November 1, 2005 **Ubuntu Security Notice, USN-224-1, December 06, 2005**	

	Sun: http://sunsolve.sun.com/search/ document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/Owl/CHANGES-current.shtml SCO: ftp://ftp.sco.com/pub/updates/ OpenServer/SCOSA-2005.23 SGI IRIX: Apply patch 5892 for IRIX 6.5.24-6.5.27: ftp://patches.sgi.com/support/free/security/patches/ Debian: http://security.debian.org/pool/updates/main/k/krb4/ Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000962 Trustix: ftp://ftp.trustix.org/pub/trustix/ updates/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-132_RHSA-2005-327.pdf FedoraLegacy: http://download.fedoralegacy.org/redhat/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/ NetBSD 2.0.3 is not vulnerable to this issue. Please contact the vendor for more information. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/k/krb4/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors IETF RFC 2406: IPSEC; Hitachi GR2000-1B, GR2000-2B, GR2000-2B+, GR2000-BH	A vulnerability has been reported that affects certain configurations of IPSec when configured to employ Encapsulating Security Payload (ESP) in tunnel mode with only confidentiality and systems that use Authentication Header (AH) for integrity protection, which could let a remote malicious user obtain plaintext IP datagrams and potentially sensitive information. Hitachi advises affected users to use the AH protocol workaround to mitigate this	IPSec ESP Packet Modification CVE-2005-0039	Medium	NISCC Vulnerability Advisory, IPSEC - 004033, May 9, 2005 US-CERT VU#302220 Security Focus, 13562, May 11, 2005 HP Security Bulletin, HPSBTU01217, August 9, 2005 **HP Security Bulletin, HPSBUX02079, December 7, 2005**

	issue. HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBTU01217&locale=en_US **HP:** **http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c00572922** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors RedHat Fedora Core4, Core3; PHP 5.0.4, 4.3.9	A remote Denial of Service vulnerability has been reported when parsing EXIF image data contained in corrupt JPEG files. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-831.html Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2 FedoraLegacy: http://download.fedoralegacy.org/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **OpenPKG:** **http://www.openpkg.org/** Currently we are not aware of any exploits for this vulnerability.	PHP Group Exif Module Remote Denial of Service CVE-2005-3353	Low	Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 RedHat Security Advisory, RHSA-2005:831-15, November 10, 2005 Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005 Fedora Legacy Update Advisory, FLSA:166943, November 28, 2005 SGI Security Advisory, 20051101-01-U, November 29, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.027, December 3, 2005**
Multiple Vendors University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7; RedHat Enterprise Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1, RedHat Desktop 4.0, 3.0, RedHat Advanced Workstation for the Itanium Processor 2.1 IA64	A buffer overflow vulnerability has been reported in the 'HTrjis()' function when handling NNTP article headers, which could let a remote malicious user execute arbitrary code. University of Kansas Lynx: http://lynx.isc.org/current/lynx2.8.6dev.14.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200510-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-803.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva:	Lynx 'HTrjis()' NNTP Remote Buffer Overflow CVE-2005-3120	High	Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005 Ubuntu Security Notice, USN-206-1, October 17, 2005 RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005 Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:186, October 18, 2005 Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005 Trustix Secure Linux Security Advisory,

	http://www.mandriva.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/l/lynx/ http://security.debian.org/pool/updates/main/l/lynx-ssl/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lynx/ (Note: Ubuntu advisory USN-206-1 was previously released to address this vulnerability, however, the fixes contained an error that caused lynx to crash.) SUSE: ftp://ftp.suse.com/pub/suse/ Slackware: ftp://ftp.slackware.com/pub/slackware/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.47 **OpenPKG:** **http://www.openpkg.org/** A Proof of Concept Denial of Service exploit script has been published.			TSLSA-2005-0059, October 21, 2005 SGI Security Advisory, 20051003-01-U, October 26, 2005 Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005 Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005 Ubuntu Security Notice, USN-206-2, October 29, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Slackware Security Advisory, SSA:2005-310-03, November 7, 2005 SCO Security Advisory, SCOSA-2005.47, November 8, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.026, December 3, 2005**
MultiTech MultiVOIP	A buffer overflow vulnerability has been reported in the SIP packet INVITE field when a string is greater than 60 characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. It has been reported that this issue was addressed in version x.08 of the software. Currently we are not aware of any exploits for this vulnerability.	MultiTech MultiVOIP Remote Buffer Overflow CVE-2005-4050	High	SecurityLab Technologies, Inc. Advisory, December 5, 2005
MXChange MXChange 0.2.0-pre3-pre10	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient	MXChange Unspecified Cross-Site Scripting & SQL Injection CVE-2005-3969 CVE-2005-3970	Medium	Secunia Advisory: SA17793, December 1, 2005

	sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://prdownloads.sourceforge.net/mxchange/mxchange-testing_0_2_0-pre_10_492.zip?download There is no exploit code required.			
MySQL AB MySQL 5.0 .0-0-5.0.4, 4.1 .0-0-4.1.5, 4.0.24, 4.0.21, 4.0.20, 4.0.18, 4.0 .0-4.0.15	A buffer overflow vulnerability has been reported due to insufficient bounds checking of data that is supplied as an argument in a user-defined function, which could let a remote malicious user execute arbitrary code. This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta available at: http://dev.mysql.com/downloads/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg Debian: http://security.debian.org/pool/updates/main/m/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/m/mysql-dfsg-4.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/universe/m/mysql-dfsg-4.1/** Currently we are not aware of any exploits for this vulnerability.	MySQL User-Defined Function Buffer Overflow CVE-2005-2558	High	Security Focus 14509, August 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:163, September 12, 2005 Ubuntu Security Notice, USN-180-1, September 12, 2005 Debian Security Advisories, DSA 829-1 & 831-1, September 30, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 Debian Security Advisory, DSA 833-1, October 1, 2005 Conectiva Linux Announcement, CLSA-2005:1023, October 6, 2005 **Ubuntu Security Notice, USN-180-2, December 05, 2005**
NetArt Media Blog System 1.2 & prior	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'cat' parameter and in 'blog.php' due to insufficient sanitization of the 'note' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Blog System Multiple SQL Injection CVE-2005-4049	Medium	Security Focus, Bugtraq ID: 15719, December 5, 2005

NetArt Media Cars Portal 1.1	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'page' and 'car' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Cars Portal Multiple SQL Injection CVE-2005-4055	Medium	Secunia Advisory: SA17914, December 6, 2005
Nodezilla Nodezilla 0.4 .0-0.4.12 -corno-fulgure	A vulnerability has been reported in the 'evl_data' private directory due to insufficient access controls, which could let a remote malicious user obtain sensitive information. Updates available at: http://www.panardvision.com.nyud.net:8090/nz/dl/nzagent-0.4.13-corno-f ulgure-linux.tgz (Linux) http://www.panardvision.com.nyud.net:8090/nz/dl/nzagent-0.4.13-corno-f ulgure-install.exe (Windows) There is no exploit code required.	Nodezilla Information Disclosure CVE-2005-4033	Medium	Secunia Advisory: SA17867, December 5, 2005
O-Kiraku Nikki O-Kiraku Nikki 1.3	An SQL injection vulnerability has been reported in 'nikki.php' due to insufficient sanitization of the 'day_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	O-Kiraku Nikki SQL Injection CVE-2005-3932	Medium	Secunia Advisory: SA17795, November 30, 2005

PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory. Upgrades available at: http://www.php.net/get/php-4.4.1.tar.gz SUSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-838.html http://rhn.redhat.com/errata/RHSA-2005-831.html Gentoo: http://security.gentoo.org/glsa/glsa-200511-08.xml Mandriva: http://wwwnew.mandriva.com/security/advisories?dis=10.2 SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **OpenPKG:** **http://www.openpkg.org/** There is no exploit code required.	PHP Multiple Vulnerabilities CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392	Medium	Secunia Advisory: SA17371, October 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005 Turbolinux Security Advisory TLSA-2005-97, November 5, 2005 Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005 RedHat Security Advisories, RHSA-2005:838-3 & RHSA-2005:831-15, November 10, 2005 Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005 Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005 SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005 SGI Security Advisory, 20051101-01-U, November 29, 2005 **OpenPKG Security Advisory, OpenPKG-SA-2005.027, December 3, 2005**
PHP-Fusion PHP-Fusion 6.0.109	An SQL injection vulnerability has been reported in 'messages.php' due to insufficient sanitization of the	PHP-Fusion SQL Injection CVE-2005-4005	Medium	Secunia Advisory: SA17871, December 5, 2005

	'srch_text' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however a Proof of Concept exploit has been published.			
phpMyAdmin phpMyAdmin 2.7.0-beta1	An HTTP response splitting vulnerability has been reported in 'Header_HTTP_Inc.php' due to insufficient sanitization of user-supplied input, which could lead to a false sense of trust. **SUSE:** **ftp://ftp.suse.com /pub/suse/** There is no exploit code required.	PHPMyAdmin HTTP Response Splitting CVE-2005-3621	Medium	Fitsec Security Advisory, November 15, 2005 **SUSE Security Summary Report, SUSE-SR:2005:028, December 2, 2005**
phpMyChat phpMyChat 0.14.6	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPMyChat Multiple Cross-Site Scripting CVE-2005-3991	Medium	Security Focus, Bugtraq ID: 15679, December 2, 2005
PHPX PHPX 3.5-3.5.9	An SQL injection vulnerability has been reported when logging into the administration section due to insufficient sanitization of the 'username' field before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPX SQL Injection CVE-2005-3968	Medium	Security Tracker Alert ID: 1015300, December 1, 2005
Pineapple Technologies Lore 1.5.4	An SQL injection vulnerability has been reported in 'article.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Lore SQL Injection CVE-2005-3988	Medium	Secunia Advisory: SA17842, December 1, 2005
PluggedOut Nexus 0.1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'search.php' due to insufficient sanitization of the 'firstname,' 'lastname,' and 'location' parameters before using in an SQL query, which could let a remote malicious user execute	PluggedOut Nexus SQL Injection & Cross-SIte Scripting CVE-2005-4056 CVE-2005-4057	Medium	Secunia Advisory: SA17909, December 6, 2005

	arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'search.php' due to insufficient sanitization of the 'firstname,' 'lastname,' and 'location' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.			
PluggedOut PluggedOut Blog 1.9.4	An SQL injection vulnerability was reported was reported in 'index.php' due to insufficient sanitization of the 'categoryid,' 'entryid,' 'year,' 'month,' and 'day' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	PluggedOut Blog SQL Injection CVE-2005-4054	Medium	Secunia Advisory: SA17911, December 6, 2005
QualityEBiz QualityPPC 1553	A Cross-Site Scripting vulnerability has been reported in the search feature due to insufficient sanitization of the 'REQ' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	QualityEBiz Quality PPC Cross-Site Scripting CVE-2005-3977	Medium	Secunia Advisory: SA17850, December 2, 2005
Quicksilver Forums Quicksilver Forums 1.1.4	An SQL injection vulnerability has been reported in the 'HTTP_USER_AGENT' header due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://prdownloads.sourceforge.net/qsforums/quicksilverforums-1.1.5.ta r.gz?download There is no exploit code required.	Quicksilver Forums SQL Injection CVE-2005-4030	Medium	Security Focus, Bugtraq ID: 15710, December 5, 2005
Real Networks RealPlayer 10.5 v6.0.12.1235, v6.0.12.1069, v6.0.12.1059, v6.0.12.1056, v6.0.12.1053, v6.0.12.1040, 10.5 Beta, v6.0.12.1016, 10.5, 10.0 BETA, 10.0 v6.0.12.690, 10.0, 8.0 Win32, 7.0 Win32, 6.0 Win32	An unspecified code execution vulnerability has been reported which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Real Networks RealPlayer Unspecified Remote Code Execution	High	eEye Digital Security, EEYEB-20051130, November 30, 2005
Relative Real Estate Systems Relative Real Estate Systems 1.2	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'mls' parameter before using in an SQL query, which could let a remote malicious	Relative Real Estate Systems SQL Injection CVE-2005-4019	Medium	Security Focus, Bugtraq ID: 15714, December 5, 2005

	user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.			
Sapid CMS Sapid CMS 1.2.3 RC2, 1.2.3	A vulnerability has been reported in the 'usr/system/insert_file.php,' 'usr/system/insert_image.php,' 'usr/system/insert_link.php,' 'usr/system/insert_qcfile.php,' and 'usr/system/edit.php' scripts due to insufficient access controls, which could let an unauthenticated remote malicious user upload files or images to a vulnerable system. Upgrades available at: http://prdownloads.sourceforge.net/sapid/sapid_v123_rc3.zip There is no exploit code required.	SAPID CMS Authentication Bypass CVE-2005-4006	Medium	Secunia Advisory: SA17859, December 2, 2005
Script Developers.NET NetClassifieds Standard Edition 1.9.6 .3, Professional Edition 1.5.1, Premium Edition 1.0.1, Free Edition 1.0.1	An SQL injection vulnerability has been reported in 'ViewCat.php' and 'gallery.php' due to insufficient sanitization of the 'CatID' parameter and in 'ViewItem.php' due to insufficient sanitization of the 'ItemNum' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	NetClassifieds Products Multiple SQL Injection CVE-2005-3978	Medium	Secunia Advisory: SA17853, December 2, 2005
sobexsrv sobexsrv 1.0 .0-pre3	A format string vulnerability has been reported in 'Dosyslog' due to insufficient sanitization of user-supplied input, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrade available at: http://www.mulliner.org/bluetooth/sobexsrv.php An exploit has been published.	Sobexsrv Dosyslog Remote Format String CVE-2005-3995	High	DMA Security Advisory, DMA2005-1202a, December 2, 2005
Sony SunnComm MediaMax 5.0.21.0	A vulnerability has been reported due to insecure default directory ACLs set on the 'SunnComm Shared' directory, which could let a malicious user obtain elevated privileges. Patch available at: http://www.sunncomm.com/support/updates/updates.asp There is no exploit code required.	Sony SunnComm MediaMax Insecure Directory Permissions CVE-2005-4069	Medium	Secunia Advisory: SA17933, December 7, 2005
SpoonLabs phpWordPress 3.0	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'poll,' 'category,' and 'ctg' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.	phpWordPress SQL Injection CVE-2005-3844	Medium	Secunia Advisory: SA17733, November 25, 2005 **Security Focus, Bugtraq ID: 15582, December 1, 2005**

	Upgrade available at: **http://www.word-press.net/patches/v30-3011-patch.zip** There is no exploit code required; however, a Proof of Concept exploit has been published.			
SugarCRM Sugar Suite 4.0 beta, 3.5	A local and remote file include vulnerability has been reported in 'acceptDecline.php,' which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	SugarCRM Sugar Suite Remote & Local File Include CVE-2005-4086 CVE-2005-4087	Medium	Security Focus, Bugtraq ID: 15760, December 7, 2005
Sun Microsystems, Inc. Java JDK 1.5.x, Java JRE 1.3.x, 1.4.x, 1.5.x / 5.x, Java SDK 1.3.x, 1.4.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error, which could let a malicious untrusted applet read/ write local files or execute local applications; three unspecified vulnerabilities were reported with the use of 'reflection' APIs error, which could let a malicious untrusted applet read/write local files or execute local applications; and a vulnerability was reported in the Java Management Extensions (JMX) implementation, which could let a malicious untrusted applet read/ write local files or execute local applications. Upgrade information available at: http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102003-1 http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102017-1 http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102050-1 Currently we are not aware of any exploits for these vulnerabilities.	Sun Java Runtime Environment Security Bypass CVE-2005-3904 CVE-2005-3905 CVE-2005-3906 CVE-2005-3907	Medium	Sun(sm) Alert Notifications Sun Alert ID: 102003, 102017, & 102050, November 28, 2005 **US-CERT VU#974188, VU#355284, VU#931684**
Sun Microsystems, Inc. Sun ONE Application Server 7.0 UR2 Upgrade Standard, 7.0 UR2 Standard Edition, 7.0 UR1 Standard Edition, ONE Application Server 7.0 Standard Edition, Java System Application Server Enterprise Edition 8.1 2005Q1RHEL2.1/ RHEL3, 8.1 2005 Q1, Java System	A man-in-the-middle vulnerability has been reported when the reverse SSL proxy plug-in is used with a supported Web server. Update information available at: http://sunsolve.sun.com/searchproxy/document.do?assetkey=1-26-102012-1 Currently we are not aware of any exploits for this vulnerability.	Sun Java System Application Server Reverse SSL Proxy Plug-in Man-In-The-Middle CVE-2005-4046	Medium	Sun(sm) Alert Notification Sun Alert ID: 102012, December 5, 2005

Application Server 7.0 2004Q2 R2 Standard, 7.0 2004Q2 R2 Enterprise, 7.0 2004Q2 R1Standard, 7.0 2004Q2 R1Enterprise, 7.0 Standard Edition, 7.0 Enterprise Edition, 7.0 2004Q2				
Tradesoft Content Management System	SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Tradesoft CMS Multiple SQL Injection CVE-2005-3987	Medium	Security Focus, Bugtraq ID: 15661, December 1, 2005
W2B phpForumPro 2.2	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'parent' and 'day' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	PHPForumPro Multiple SQL Injection CVE-2005-4088	Medium	Security Focus, Bugtraq ID: 15736, December 6, 2005
W3C Libwww 5.4	Multiple unspecified vulnerabilities have been reported including a buffer overflow and vulnerabilities related to the handling of multipart/byteranges content. The impact was not specified. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/w/w3c-libwww/** Currently we are not aware of any exploits for these vulnerabilities.	W3C Libwww Multiple Unspecified Vulnerabilities CVE-2005-3183	Not Specified	Fedora Update Notifications, FEDORA- 2005-952 & 953, October 7, 2005 Mandriva Linux Security Advisory, MDKSA-2005:210, November 10, 2005 **Ubuntu Security Notice, USN-220-1, December 01, 2005**
Web Calendar WebCalendar 1.0.1	An HTTP response splitting vulnerability has been reported in 'Layers_Toggle.php' due to insufficient sanitization, which could let a remote malicious user influence or misrepresent how Web content is served, cached or interpreted. **Patches available at:** **https://sourceforge.net/tracker/download.php?group_id=3870&atid=303870 &file_id=158009 &aid=1369439**	WebCalendar HTTP Response Splitting CVE-2005-3982	Medium	Security Focus, 15673, December 1, 2005

	There is no exploit code required; however, a Proof of Concept exploit has been published.			
Web4Future Inc. Web4Future Affiliate Manager PRO 4.1	An SQL injection vulnerability has been reported in 'functions.php' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Web4Future Affiliate Manager PRO SQL Injection CVE-2005-4037	Medium	Security Focus, Bugtraq ID: 15717, December 5, 2005
Web4Future Inc. Web4Future eDating Professional 5.0 & prior	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 's,' 'pg,' and 'sortb' parameters; in 'gift.php' due to insufficient sanitization of the 'cid' parameter; and in 'articles.php' due to insufficient sanitization of the 'fq.php,' and 'cat' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Web4Future eDating Professional SQL Injection CVE-2005-4034	Medium	Secunia Advisory: SA17879, December 5, 2005
Web4Future Inc. Web4Future Portal Solutions	Several vulnerabilities have been reported:an SQL injection vulnerability was reported in 'comentarii.php' due to insufficient sanitization of the 'idp' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'arhiva.php' due to insufficient verification of the 'dir' parameter before used to list files & directories, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Web4Future Portal Solutions Information Disclosure & SQL Injection CVE-2005-4038 CVE-2005-4039	Medium	Secunia Advisory: SA17880, December 5, 2005
WebCalendar WebCalendar 1.0.1	Several vulnerabilities have been reported: SQL injection vulnerabilities were reported due to insufficient sanitization of 'export_handler.php,' 'activity_log.php,' 'admin_handler.php,' and 'edit_template.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'export_handler.php' due to insufficient verification of the 'id' and 'format' parameters before used to save data files, which could let a remote malicious user overwrite saved data files. No workaround or patch available at time of publishing.	WebCalendar SQL Injection & File Overwrite CVE-2005-3949 CVE-2005-3961	Medium	Secunia Advisory: SA17784, November 29, 2005 **Security Focus, Bugtraq ID: 15606, December 1, 2005**

	There is no exploit code required.			
Widget Press Widget Property 1.1.19	SQL injection vulnerabilities have been reported in 'property.php' due to insufficient sanitization of the 'property_id,' 'zip_code,' 'property_type_id,' 'price,' and 'city_id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however Proof of Concept exploits have been published.	Widget Press Widget Property SQL Injection CVE-2005-4016 CVE-2005-4017	Medium	Security Focus, Bugtraq ID: 15701, December 5, 2005
WinEgg DropShell WinEgg DropShell 1.7 (Remote Access Trojan)	Multiple remote buffer overflow vulnerabilities have been reported: a buffer overflow vulnerability was reported that affects the HTTP server when a GET request is provided that contains excessive data, which could let a remote malicious user execute arbitrary code; and two buffer overflow vulnerabilities were reported that affect the FTP server when FTP commands are provided that contain excessively long arguments, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	WinEggDrop Shell Multiple Remote Buffer Overflows CVE-2005-3992	High	Security Focus, Bugtraq ID: 15682, December 2, 2005
WSN Knowledge Base WSN Knowledge Base 1.2 .0	SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'catid,' 'perpage,' 'ascdesc,' and 'orderlinks' parameters and in 'comments.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	WSN Knowledge Base Multiple SQL Injection CVE-2005-3939	Medium	Security Focus, Bugtraq ID: 15656, November 30, 2005
Xaraya Xaraya 1.0 RC1-RC4	A Directory Traversal vulnerability has been reported in the 'index.php' script 'module' parameter, which could let a remote malicious user obtain sensitive information. **Patch available at: http://www.xaraya.com/downloads/patches/xarsecurity051130.zip** There is no exploit code required; however, a Proof of Concept exploit has been published.	Xaraya Directory Traversal CVE-2005-3929	Medium	Security Focus, Bugtraq ID: 15623, November 29, 2005 **Security Focus, Bugtraq ID: 15623, December 1, 2005**
Zen Cart Team Zen Shopping Cart 1.2.6 d	An SQL injection vulnerability has been reported in 'admin/password_forgotten.php' due to insufficient	Zen Cart SQL Injection CVE-2005-3996	Medium	Security Tracker Alert ID: 1015306, December 2, 2005

	sanitization of the 'admin_email' parameter before using an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrade available at: http://www.zen-cart.com/modules/mydownloads/ There is no exploit code required; however a Proof of Concept exploit script has been reported.

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Mobile Anti-Virus: Now or Later?** Experts point to gathering clouds of viruses and Trojans but the fact is that security architects, particularly those in the United States, have little to fear for now. Employees are introducing smartphones and PDAs into the corporate network at the same time the number of smartphone Trojans and viruses is rising. Malware writers are experimenting with new propagation methods and more malicious payloads. Source: http://www.mobilepipeline.com/174403206;jsessionid=5VLIYULCKOEGYQSNDBOCKH0CJUMEKJVN.
- **Bluetooth roadmap updated but UWB wars could scupper it:** The Bluetooth Special Interest Group, which controls the development of the short range wireless standard, will publish an updated roadmap that defines plans up to the third quarter of 2007 shortly. The focus will be on interoperability with UltraWideBand (UWB). Source: http://www.theregister.com/2005/12/06/bluetooth_roadmap/.
- **Wireless Hackers 101:** Attacks on wireless LANs (WLANs) and wireless-enabled laptops are a quick and easy way for hackers to steal data and enter the corporate network. IT departments must have a pre-emptive plan of action to prevent these malicious and illegal attacks, which compromise an organization's data privacy and can wreak havoc on network infrastructure. Source: http://www.esecurityplanet.com/prevention/article.php/3568071.

Wireless Vulnerabilities

- Sobexsrv Dosyslog Remote Format String: A format string vulnerability has been reported in 'Dosyslog' due to insufficient sanitization of user-supplied input.
- sobexsrv.pl.txt: Remote exploit for the sobexsrv format string vulnerability.
- BluePIMped.txt: A write up on the exploitation of the Widcomm BTStackServer used for Bluetooth connectivity.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
December 7, 2005	appfluent_db_ids_exp.c	No	Exploit for the Appfluent Technology Database Buffer Overflow vulnerability.
December 7, 2005	BluePIMped.txt	N/A	A write up on the exploitation of the Widcomm BTStackServer used for Bluetooth connectivity.
December 7, 2005	john-1.6.39w-mmx.zip	N/A	A fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, and BeOS. Its primary purpose is to detect weak Unix passwords, but a number of other hash types are supported as well.
December 7, 2005	sobexsrv.pl.txt	No	Exploit for the Sobexsrv Dosyslog Remote Format String vulnerability.
December 7, 2005	SugarSuite_poc	No	Proof of Concept exploit for the SugarCRM Sugar Suite Remote and Local File Include vulnerability.
December 6, 2005	docebo_204_xpl.php	No	Proof of Concept exploit for the DoceboLMS Arbitrary File Upload Vulnerability.
December 6, 2005	horde-imp_html-inj-poc.pl	No	Proof of Concept exploit for the Horde IMP Email Attachments HTML Injection Vulnerability.
December 3, 2005	iwar-0.06.tar.gz	N/A	A war dialer written for Unix type (Linux/OpenBSD/etc) operating systems.
December 3, 2005	iwar-0.06-DOS.zip	N/A	A war dialer written for Unix type (Linux/OpenBSD/etc) operating systems.
December 3, 2005	pbnj-1.10.tar.bz2	N/A	A network tool that can be used to give an overview of a machine or multiple machines and includes the details about the services running on them.

December 3, 2005	perl-format-string.txt	N/A	Whitepaper that discusses the attack and impact details of recent discussions surrounding format string exploitation in perl.
December 3, 2005	StackBasedOverflows-Windows-Part3.pdf	N/A	Writing Stack Based Overflows on Windows - Part III: Walking through a stack based overflow and writing an exploit for a local overflow.
December 3, 2005	StackBasedOverflows-Windows-Part4.pdf	N/A	Writing Stack Based Overflows on Windows - Part IV: Shellcode creation and exploitation an application remotely.
December 3, 2005	StackOverflow-Examples.txt	N/A	Source code for all the examples used in tutorials 1 through 4 of 'Writing Stack Based Overflows On Windows'.
December 2, 2005	n13SQL.php.txt	No	Exploit for the N-13 News SQL Injection vulnerability.
December 2, 2005	phpX_359_xpl.php phpx_359_xpl.txt	No	Proof of Concept exploit for the PHPX SQL Injection vulnerability.
December 2, 2005	webCalSQL.txt	No	Exploit details for the WebCalendar SQL Injection vulnerability.
December 2, 2005	WinEggDropShell_bof.py AD20051202.txt	No	Proof of Concept exploit for the WinEggDropShell Multiple Remote Buffer Overflow vulnerabilities.
December 2, 2005	xarayaDOS.txt	No	Exploit details for the Xaraya Directory Traversal vulnerability.
December 2, 2005	zencart_126d_xpl.php zencart_126d_xpl.html	No	Proof of Concept exploit for the Zen Cart SQL Injection vulnerability.
December 1, 2005	55k7-msdtc.c msdtc.cpp	Yes	Proof of Concept exploit for the Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service vulnerability.
December 1, 2005	gdsexploit.html	No	Proof of Concept exploit for the Microsoft Internet Explorer CSS Import Cross-Domain Restriction Bypass Vulnerability.
December 1, 2005	guppy459_xpl.txt	No	Script that exploits the GuppY Remote File Include & Command Execution vulnerabilities.
December 1, 2005	ieDoS.pm.txt	Yes	Exploit for the Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service vulnerability.
December 1, 2005	phgrafx.txt	No	Script that exploits the QNX Phgrafx Buffer Overflow vulnerability.
December 1, 2005	win_dos.c winCreateExp.txt	No	Exploit for the Microsoft Windows CreateRemoteThread Local Denial of Service vulnerability.

[back to top]

Trends

- **Automatic Update Functionality in Sober.X Worm:**US-CERT is aware of functionality that could allow the mass-mailing worm known as "W32/Sober.X" to automatically update itself. W32/Sober.X is a bi-lingual (English and German) mass-mailing worm that utilizes its own SMTP engine to propagate. Source: http://www.us-cert.gov/current/.
- **Perl programs providing user-controlled I/O format strings may contain format string vulnerabilities:** Programs written in Perl may contain many of the same types of format string vulnerabilities that programs written in C can contain. US-CERT VU#946969
- **Exploit for Vulnerability in Microsoft Internet Explorer window() object**: US-CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles requests to the window() object. Source: http://www.us-cert.gov/current/
- **Reports of IRS Phishing Emails:** US-CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax-refunds@irs.gov". Source: http://www.us-cert.gov/current/.
- **Trojans target unpatched IE flaw:** Several Trojan horses that exploit an unpatched flaw in Internet Explorer have been discovered. According to Sophos two exploits, Clunky-B and Delf-LT, could allow malicious code to be executed remotely on a user's PC. These Trojans could "download anything, including a 'banker Trojan' that gives up your bank details." Source: http://news.zdnet.co.uk/0,39020330,39240189,00.htm
- **November breaks all malware records:** According to the antivirus firm, Sophos, November was the worst month for malware since records began in the mid-1980s. They detected 1,940 new pieces of malware in the past month, and have seen a 48 per cent increase in threats over the year. Source: http://www.vnunet.com/vnunet/news/2147200/november-biggest-ever-malware.
- **Holiday spam could reach one billion emails:** According to email security vendor, MailFrontier, the number of spam and phishing messages could top 1 billion this Christmas. Last year 750 million emails were sent over the Christmas period, with both bogus sales offers and phishing attacks. Source: http://www.vnunet.com/vnunet/news/2147012/holiday-spam-reach-billion.
- **IT spending overtaken by compliance issues:** According to Gartner, money spent on IT to ensure compliance with regulations will outweigh money spent on new technologies. The research, which assessed trends that will impact people, business and the IT industry, found that this pattern will continue through until 2010, with regulatory compliance IT spending growing at twice the rate of general IT spending. Source: http://www.vnunet.com/crn/news/2147155/spending-overtaken-compliance.
- **Cyber criminals gather on forgotten Web sites:** According to security experts, cyber criminals selling programs to hack into computers and stolen bank account numbers are moving to abandoned Web sites where their activities are harder to track. Dormant Web sites no longer monitored by administrators have in effect created hundreds of online bazaars for criminals. Source: http://www.msnbc.msn.com/id/10284366/from/RSS/.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Netsky-D	Win32 Worm	Slight Increase	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
3	Sober-Z	Win32 Worm	New	December 2005	A mass-mailing worm that harvests addresses from infected machines, forges the senders email, and utilizes its own mail engine.
4	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender’s address.
5	Mytob.C	Win32 Worm	Increase	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
6	Mytob-BE	Win32 Worm	Decrease	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	Zafi-D	Win32 Worm	Slight Increase	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
8	Lovgate.w	Win32 Worm	Slight Decrease	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
9	Mytob-GH	Win32 Worm	New	December 2005	This email worm turns off anti-virus and opens infected systems to remote connections. It further harvests email addresses from infected machines, and forges the senders address.
10	Zafi-B	Win32 Worm	Slight Decrease	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.

Table updated December 5, 2005

[back to top]

Last updated December 08, 2005